

## بررسی و مقایسه‌ی معماری‌های امنیتی رایانش ابری در راستای ارائه راهکارهایی جهت توسعه سازمان‌های امنیتی

زهرا سلیمی<sup>۱</sup>

<sup>۱</sup> کارشناسی ارشد مهندسی نرم‌افزار و استاد حق التدریسی دانشگاه پیام نور واحد کرمانشاه

### چکیده

رایانش ابری یک مقوله مهم در عصر نوین فناوری اطلاعات بدل شده است. از این رو جدیدترین تحقیقات در این حوزه پیرامون فناوری ابری صورت می‌گیرد. به همین دلیل شناخت چالش‌های پیرامون رایانش ابری از اهمیت بالایی برخوردار است. مفاهیم تعامل پذیری، امنیت، استانداردسازی و معماری‌های امنیتی مهم‌ترین چالش‌های فضای ابری هستند. از این رو، این مقاله با هدف بررسی معماری امنیتی رایانش ابری در سازمان‌های امنیتی سعی در توسعه مفاهیم امنیتی رایانش ابری دارد. به همین دلیل در ابتدا معماری‌های مختلف رایانش ابری تعریف و بررسی شده است. سپس با بررسی نقاط ضعف و قوت معماری‌های پیشنهادی، با ارائه راهکارهایی به توسعه سازمان‌های امنیتی در راستای بهبود معماری امنیتی رایانش ابری پرداخته شده است.

**واژه‌های کلیدی:** رایانش ابری، معماری امنیتی، سازمان‌های امنیتی، معماری رایانش ابری

## ۱. مقدمه

اگرچه ظهور رایانش ابری یک پیشرفت متأخر بشمار می آید، درک جنبه های حساس امنیتی می تواند از تجارب گزارش شده سازگارترهای اولیه و همچنین از محققین که سکوه های ایجادگر ابری موجود و فناوری های دست اندرکار را تحلیل و آزمایش می کنند، جمع آوری شود. بخش های ذیل مسئله مربوطه به امنیت و حریم خصوصی را مشخص می کند که پنداشته می شود اهمیت بلندمدتی به رایانش ابری عمومی و در بسیاری از موارد به سایر مدل های سرویس رایانش ابری می دهند. در برخی از موارد این احتمال می رود که نمونه های مشکلات تعریف شده یا مشخص شده پیشین برای طرح مسئله ای ارائه نمودند. نمونه ها جامع نیستند و ممکن است که یک جنبه از یک موضوع کلی تر را پوشش دهند. در مسائل بسیاری، مشکلات خاص مطرح شده دوباره طرح و حل گشته اند. با این وجود مسئله وسیع تر در اکثر موارد از خود سماعت و مقاومت نشان می دهد و دارای پتانسیلی است که از راه های دیگری دوباره خود را در میان مدل های سرویس مختلف بروز دهد. ملاحظات امنیتی و حریم خصوصی که از برون داد فناوری اطلاعات منقطع می شوند، نیز وجود دارد. در ادامه به بررسی معماری، امنیت و دفاع پرداخته شده است [۱].

امنیت و حریم خصوصی کاربران، برنامه های کاربردی، دستگاه ها، منابع شبکه و داده ها بخش های بسیار مهم معماری و طراحی آن هستند. امنیت در همه بخش های معماری تلفیق شده و بر سایر کارکردها در معماری و معماری های مبتنی بر شبکه اثر می گذارد. واجب است برای کارکرد مناسب امنیت در این حوزه، روابط بین سازوکارهای امنیتی و همچنین روابط بین معماری امنیت و دیگر اجزای معماری به خوبی شناسایی شوند [۳].

فضای مجازی یک سکوی دیجیتالی است که همه افراد، سازمان ها، نهادهای دولتی و شرکتی را در محیط اطلاعاتی بهم پیوند می دهد و در همه حوزه های فیزیکی نفوذ می کند و اساس و بنیان همه عملیات ها است. در یک محیط امنیتی آینده که با پیچیدگی و ابهام همراه است، نیروی های امنیتی پیوند ناگشودنی با توانایی فعالیت موثر وزارت دفاع در فضای مجازی خواهند داشت. در شرایط فعلی سیاسی، اقتصادی و تکنولوژی، از فناوری اطلاعات انتظار می رود قابلیت های بیشتری در حالی که منابع کمتری مصرف می کند، ارائه دهد. با افزایش حمایت های دولتی و تهدیدات امنیتی مستقل، دپارتمان های امنیتی اهمیت روزافزون یک فضای امنیتی امن و محکم را شناسایی می کند. در حال حاضر هم زمان رویدادهای مالی جهان یک نیاز جدید را ایجاد می کنند که سخت گیری های بیشتری پیرامون مسائل مالی و اشتباهات مالی اعمال می نماید. در نتیجه، این دپارتمان می بایست راه های به دست آوردن، عمل کردن و مدیریت فناوری اطلاعات را تغییر دهد تا افزایش بهره وری، تأثیر گذاری و امنیت را درک کند. دپارتمان های امنیتی جهت پیشبرد اهداف خود باید به بررسی مسائل روز فضای مجازی بپردازند. از این رو، استراتژی رایانش ابری یک عامل مهم در این حوزه است و شاخص های آن در محیط سازمان ابری باید لحاظ شود [۳، ۴].

دولت، صنعت و دیگر ذینفعان باید الزامات را تعریف کنند، استانداردهای امنیت، تعامل متقابل و قابلیت انتقال داوطلبانه بین المللی مبتنی بر توافق را توسعه دهند، و آن ها را در محصولات، فرایندها، و خدمات اجرا و پیاده سازند. (استانداردهای امنیت، تعامل متقابل و قابلیت انتقال). محصولات، فرایندها و خدمات مبتنی بر استانداردها برای سازمان های دولت آمریکا<sup>۱</sup> لازم و اساسی هستند تا اطمینان دهند که [۱، ۵]:

- سرمایه گذاری های عمومی بزرگ بالقوه دچار کهنگی فناوری زود هنگام نمی شوند،
- سازمان های دولتی قادر به تغییر ارائه دهندگان خدمات ابر هستند که می توانند از مأموریت هایشان به صورت انعطاف پذیر و مقرون به صرفه پشتیبانی کنند، و
- دولت آمریکا از یک میدان اقتصادی هموار برای ارائه دهندگان خدمات پشتیبانی می کند.

توسعه استانداردها با شناسایی الزامات مشخص و روشن، آغاز می شود. سازمان های USG الزاماتی مربوط به مأموریت را شناسایی کرده اند بستگی به استانداردهای امنیتی، قابلیت انتقال و تعامل متقابل فنی دارند. گروه کاری عمومی نقشه

<sup>۱</sup> United States Government (USG)

استانداردهای رایانش ابر NIST، استانداردهای فناوری اطلاعات کلی را فهرست کرده است که برای رایانش ابر استفاده می‌شوند، و استانداردهای نوظهوری که الزامات مختص فناوری‌های زیربنایی را هدف قرار می‌دهند که امکان رایانش ابری را فراهم می‌کند. این تلاش تنها سه استاندارد ابری نوظهور را تاکنون شناسایی کرده است، اگرچه سازمان‌های استانداردها در حال اتخاذ استانداردهای دیگری هستند. یافته‌های پروژه تسریع استانداردهای NIST جهت راهاندازی اتخاذ رایانش ابری نمونه‌های کاری را ارائه می‌دهد که نشانگر چگونگی پشتیبانی از پرونده‌های مهم استفاده فنی در سیستم‌های ابری است که ویژگی‌های سیستم ابر عمومی و ثبت شده را اجرا می‌کند. تسریع استانداردها جهت راهاندازی اتخاذ رایانش ابری دریافت که موارد استفاده فنی امنیتی، قابلیت انتقال، و تعامل متقابل بسیار بهم متصل و مرتبط اند، و نیاز به استانداردهای امنیتی، تعامل متقابل و قابلیت انتقال داوطلبانه بین‌المللی مبتنی بر توافق یکپارچه را برجسته می‌کنند [۵، ۱].

در شرایط فعلی سیاسی، اقتصادی و تکنولوژی، از فناوری اطلاعات انتظار می‌رود قابلیت‌های بیشتری درحالی‌که منابع کمتری مصرف می‌کند، ارائه دهد. با افزایش حمایت‌های دولتی و تهدیدات امنیتی مستقل، دپارتمان‌های امنیتی اهمیت روزافزون یک فضای امنیتی امن و محکم را شناسایی می‌کند. در حال حاضر هم‌زمان رویدادهای مالی جهان یک نیاز جدید را ایجاد می‌کنند که سخت‌گیری‌های بیشتری پیرامون مسائل مالی و اشتباهات مالی اعمال می‌نماید. در نتیجه، این دپارتمان می‌بایست راه‌های به دست آوردن، عمل کردن و مدیریت فناوری اطلاعات را تغییر دهد تا افزایش بهره‌وری، تأثیرگذاری و امنیت را درک کند. دپارتمان‌های امنیتی جهت پیشبرد اهداف خود باید به بررسی مسائل روز فضای مجازی بپردازند. از این‌رو، استراتژی رایانش ابری یک عامل مهم در این حوزه است و شاخص‌های آن در محیط سازمان ابری باید لحاظ شود [۵، ۱].

در ادامه این مقاله بخش دوم به بررسی مفهوم رایانش ابری؛ بخش سوم به بررسی استراتژی رایانش ابری؛ بخش چهارم به بررسی معماری رایانش ابری و مباحث امنیتی در معماری رایانش ابری پرداخته است. در ادامه بخش پنجم به بررسی و ارائه راهکارهای معماری امنیتی رایانش ابری پرداخته است. در نهایت، نتیجه‌گیری مقاله ارائه شده است.

## ۲. رایانش ابری

در دیدگاه‌های مختلف یک معماری ۳ لایه‌ای و یک معماری ۴ لایه‌ای معرفی شده است. این معماری دارای ۳ لایه اصلی است و لایه زیر ساختار خود را به یکی از سه زیر لایه تبدیل کند. نخستین بار معماری بخش CaaS مطرح شده است و به برخی قابلیت‌های ارتباطی که از طریق شبکه‌های ابری اشاره دارد. در لایه‌ها، هر لایه زیر بنایی برای لایه بالایی خود است و اشکال مختلفی در رابطه با خدمات محاسبات ابری وجود دارد درواقع نوعی از منابع است که از طریق اینترنت در اختیار مشتریان قرار می‌گیرد. سلسله‌مراتب محاسبات ابری که به‌صورت شکل ۱ ارائه می‌گردد شامل موارد زیر است [۲]:

۱. سرویس نرم‌افزار ابری
۲. سرویس به‌عنوان بستر ابری
۳. سرویس به‌عنوان زیرساخت ابری
۴. مراکز داده‌ها

اگر از سمت مدل استقرار برنامه در سطح سازمانی به یکی از مدل‌های ابری برویم، بایستی در خصوص معماری‌های رایانش ابری مطالعه بیشتری بکنیم. ابرهای خصوصی و عمومی ویژگی مشابهی دارند. در کل سه نوع مدل خدمات اصلی وجود دارد که باید در نظر گرفت. سازمان‌های فناوری اطلاعات برنامه‌های خود را بر طبق کاربردهای عمومی، خصوصی یا ترکیبی قرار دهند. اطلاعات عمومی، خصوصی و ترکیبی به مکان وابستگی ندارند. معمولاً ابرهای عمومی در اینترنت و ابرهای خصوصی در یک محدوده خاص می‌باشند. ابرهای خصوصی در فضاهای اشتراکی نیز می‌توانند قرار گیرند. شرکت‌ها در انتخاب مدل رایانش ابری خود نکات زیادی را موردتوجه قرار می‌دهند. مثلاً برای یک مسئله، مدل‌های گوناگونی را بکار

می گیرند. برای قرارگیری در ابر عمومی به یک برنامه کاربردی موقتی نیاز است، زیرا نیاز به خرید تجهیزات اضافی را یک نیاز موقتی برطرف می کند؛ بنابراین، یک برنامه ای که نیازمند کیفیت خدمات است، یا اینکه نیازمند مکان داده از نظر جغرافیایی است، بهتر است که در یک ابر خصوصی یا ترکیبی باشد. جدول ۱ توضیحاتی کلی از لایه های سلسله مراتبی رایانش ابری را نشان داده است [۶].



شکل ۱ - سلسله مراتب لایه های محاسبات ابری [۶]

الزامات مورد بحث در این بخش از نقشه فناوری رایانش ابری USG به این صورت شناسایی می شوند: الزمات امنیتی، تعامل متقابل و قابلیت انتقال راهبردی و تاکتیکی با اولویت بالا که سازمان های USG باید به آنها دست یابند تا مدل رایانش ابری را جهت دستیابی به اهداف استراتژی رایانش ابری اتخاذ کند [۵].

جدول ۱ - خصوصیات، خدمات و سازمان ارائه کننده: لایه های سلسله مراتبی رایانش ابری [۵]

نوع	خصوصیات	برخی از خدمات	سازمان های ارائه کننده
نرم افزار به عنوان سرویس	نرم افزار به عنوان خدمات، خدمات مبتنی بر تقاضای مشتری، ارائه خدمات به چندین کاربر بصورت همزمان، اجرا کلیه خدمات بر روی محیط ابر	ذخیره سازی، پست الکترونیک، بازارهای الکترونیکی راه دور، اشتراک داده تصویر، مدیریت فرآیند کسب و کار	Gmail Drive Zimory.com SmugMug Appian Anywhere
سکو به عنوان سرویس	مبتنی بر استفاده، قابلیت فاز بندی در پروسه های پیاده سازی، قابلیت شبیه سازی بر روی بسترهای مجازی سازی سیستم عامل، مشتری با سکو از طریق API قادر است ارتباط برقرار کند.	داده، پایگاه سازی، ذخیره محاسبات، پرداخت، صدور صورت حساب	Amazon EC۲, EC۳, SimpleDB, Network.com, salesforce
زیرساخت به عنوان سرویس	قابلیت های محاسباتی و ذخیره سازی در این لایه فراهم میشود. حجم کاری و سایر نیازهای اساسی برنامه های کاربردی در این قسمت تامین میشود.	خدمات زیر ساخت از جمله سرورها، سیستم های ذخیره سازی، سوئیچ ها، روترها	Xcalibre FlexiScale Joyenet

## ۳. استراتژی رایانش ابری

برای برنامه ریزی آینده، هر سه مدل عمده تحویل (IaaS, PaaS, and SaaS) در اینجا می مانند. همان طور که مشتریان درمی یابند که ارزش و منابع ذخیره های بیشتری از سرویس های نرم افزار و سکو بجای زیر ساختار وجود دارد، محتمل است که IaaS سهم بازار به تدریج افت می کند. اگرچه وابستگی ها و فاکتورهای تکنیکی خاص سرویس های ابری IaaS شناور را برای مدتی نگه می دارد تا به مرحله انجام برسند. احتمالاً ما استحکام بیشتری را در فضای IaaS خواهیم دید زیرا بازار سرویس ابری IaaS مانعی بسیار خفیف برای ورود و ضریب کمترین تفکیک تکنیکی دارد. همان طور که IaaS کالایی تجاری می شود، بازگشت سرمایه افت می کند و ایجادگرهای ابری مجبور به نقل مکان به بخش های پرمفعت تر PaaS و SaaS می شوند. ایجادگرهای خرده پا IaaS منابع مالی ندارند تا نرم افزار پیچیده را توسعه دهد تا در فضای PaaS و SaaS رقابت کنند و بنابراین استحکامات و شراکت ها برای ادامه حیات لازم خواهد بود. توسعه PaaS و سرویس های کیفیت بالا به شرکت ها کمک می کنند تا کیفیت کد را بهبود بخشند، همکاری تیم توسعه را ارتقاء دهند و توسعه نرم افزار و چرخه یکپارچه سازی مداوم را تسریع کنند. اکثر گروه های توسعه ترجیح می دهند از روش توسعه نرم افزار چابک در مقابل مدل آبشاری سنتی استفاده کنند. سکوه های توسعه PaaS و ابزارهای همکاری شرکت ها را با پس اندازهای اساسی پولی و زمانی تأمین می کند و بنابراین ما احتمالاً ابداعات بیشتری رو در این بخش خواهیم دید. تحلیل داده و اطلاعات تجارت ابری به عنوان یکی از سودمندترین بخش ها در بازار سرویس های ابری باقی می ماند [۱، ۲].

صنعت باید خدمات ابر را همواره و به وضوح طبقه بندی کند (فناوی و هدایت قابلیت انتقال و تعامل متقابل). از این رو، استراتژی رایانش ابری بدین صورت قابل تحقق است [۶]:

الف) مشتریان پیچیدگی های انواع مختلف خدمات ابر را درک کنند و بهتر بتوانند خدمات ابر مناسب را برای رسیدن به اهداف کسب و کارشان انتخاب کنند،

ب) مشتریان قادر خواهند بود بین محصولات فروشندگان ابر مختلف، ارزیابی و مقایسه و انتخاب کنند، و

ج) برای ارائه دهندگان مشخص خواهد شد که چه موقع قابلیت انتقال و تعامل متقابل باید در طبقه بندی های مشابه خدمات ابر وجود داشته باشند.

تعریف رایانش ابری NIST سه طبقه بندی مجزای مدل های خدمات ابر را شناسایی کرده است: نرم افزار به عنوان یک خدمت، پلتفرم به عنوان یک خدمت، و زیرساخت به عنوان یک خدمت. در حال حاضر، مصرف کنندگان باید به دنبال درک خدمات ابری از طریق دیدگاه سفارشی ارائه شده توسط هر ارائه دهنده خدمات باشند. به علاوه، درحالی که بسیاری فروشندگان به دنبال ایجاد طبقه بندی های جدید از خدمات هستند، که موقعیت بازارشان را بهبود ببخشند، مشخص نیست که هر یک از طبقه بندی های پیشنهادی منحصر به فرد است و در سه خدمت اولیه موجود قرار ندارد. نمونه های مواداضافه شده پیشنهادی شامل داده به عنوان یک خدمت، شبکه به عنوان یک خدمت، خدمت به عنوان یک خدمت، و غیره است. نتیجه آن چشم انداز گیج کننده ای از خدمات ابری بالقوه است [۱، ۲].

در اواخر سال ۲۰۱۰، تیم پروژه معماری مرجع رایانش ابری NIST، ۱۱ مدل مرجع رایانش ابری موجود پیشنهادی سازمان های ابر، فروشندگان، و سازمان های اتحادی (فدرال) را بررسی کرد تا ببیند که آیا توافق صنعتی مشخصی بین آنها وجود دارد. تحلیل نشانه اختلاف گسترده ای بود. مشتریان به یک مدل بی طرف مورد درک عموم نیاز دارند تا همواره و مشخصاً درک کنند که چگونه خدمات ابری مقایسه می شوند (برای مثال اپل با اپل). در نوامبر ۲۰۱۰، گروه کاری عمومی به میزبانی NIST شروع به بررسی معماری های مرجع نمود و همه توصیه های پیشنهاد را بررسی کرد. گروه این کار را از طریق اتفاق نظر تلفیق به پیش برد تا معماری مرجع بی طرف را تعریف کند. معماری مرجع اولیه و طبقه بندی بر "کدام" در مقابل "چگونگی" پیاده سازی و اجرا تمرکز دارد، و محدود به اجرا و پیاده سازی یک فروشنده خاص نیست. اگرچه شرکت کنندگان صنعتی این مدل را با طرح ریزی آن در خدمات ابری شان، تایید نموده اند، تا برای USG و سایر مصرف کنندگان مفید باشد، تایید و مشارکت گسترده تر ذینفعان مورد نیاز است [۵، ۶].

## ۴. معماری رایانش ابری

معماری نرم افزار و سخت افزار بکار رفته در تحویل سرویس های ابری می تواند بطور بسزایی در میان ایجادگرهای ابری عمومی برای هر مدل خاصی از سرویس متفاوت باشد. موقعیت فیزیکی زیر ساختار توسط ایجادگر ابری تعیین می شود، همانطور که آن زیر ساختار، طرح و پیاده سازی قابلیت اتکاء ادغام منابع، مقایس پذیری و سایر منطق مورد نیاز در چهار چوب پشتیبان است. برنامه های کاربردی بر مبنای واسطه های برنامه نویسی سرویس های اینترنت دسترس پذیر شکل می گیرند که عمده تاً اجزای ابری چندگانه را با یکدیگر در پیرامون برنامه های کاربردی برنامه ریز واسطه ها درگیر می کنند. ماشین های مجازی اصولاً بعنوان واحد انتزاعی دخل و تصرف برای ابرهای IaaS بکار می رود و بصورت نا هماهنگی با معماری ذخیره ابری جفت و جور می شود. ایجادگر ابری همچنین سایر کیفیات انتزاعی محاسباتی در عوض فناوری ماشین مجازی به منظور تدارک سرویس ها برای هر مدل سرویسی دیگر می تواند، استفاده شود [۷].

برای پیاده سازی سمت سرور معادله، برنامه های ابر محور به سمت مشتری معادله نیاز دارند تا سرویس ها را راه اندازی و کسب کنند. درحالیکه مرورگرهای شبکه اغلب بعنوان مشتری خدمت می کنند، سایر احتمالات حذف می شود. علاوه بر آن زیر ساختار ارتباطات شبکه امن و دقیق باید در مکان مناسب قرار گیرند، بسیاری از واسطه های ساده سازی شده و کیفیات انتزاعی سرویس در مورد مشتری سرور و شبکه مبتنی بر پیچیدگی ذاتی است که بر قضیه حریم خصوصی و امنیت تأثیر می گذارد. بنابراین حائز اهمیت است که تکنولوژیهای ایجادگر ابری استفاده می کند تا سرویس ها را تدارک بیند، به درستی درک شوند و کنترل های تکنیکی مربوطه، دلالت هایی بر امنیت و حریم خصوصی سیستم در سراسر چرخه عمرش دارند. با چنین اطلاعاتی معماری سیستمی بنیادین ابر می تواند تجزیه شود و بصورت چارچوبی از کنترل های امنیتی و حریم خصوصی که در ارزیابی و مدیریت بحران بکار می رود، طراحی شوند [۷].

معماری مرجع (CCRA)، یک طرح تخصصی برای سیستم هایی که با دیدگاهی مناسب تعریف شده اند، ارائه می کند و همچنین نیازها را تأمین و تصمیمات معماری رو محقق می سازد. این مدل برای پروژه های پیشرفته دو مقوله سازگاری و کیفیت را ارائه و تضمین می کند. معماری مرجع رایانش ابری IBM طرحی برای خدمات ابری است که منابع و استفاده از نیروی کار را بهینه سازی نموده و طی عملیاتی به مقیاس اقتصادی دست می یابد. معماری مرجع رایانش ابری IBM مبتنی بر ورودی حقیقی مبتنی بر راه اندازی های ابری درون IBM است. این معماری اجزای بنیادی را تعریف کرده و راهنمایی هایی برای ساخت محیط ابری ارائه و پشتیبانی می کند. معماری IBM از سه نقش اصلی تشکیل شده است که شامل مشتری (مصرف کننده) سرویس ابری، تأمین کننده سرویس ابری و سازنده سرویس ابری است. هر نقش می تواند توسط یک نفر یا گروهی از افراد یا توسط یک یا چند سازمان تحقق یابد [۱، ۷، ۸].

مشتری خدمات ابری یا یک سازمان، عامل انسانی یا سیستم IT است که مواردی از خدمات ارائه شده توسط تأمین کننده سرویس ابری خاص را مصرف می کند. علاوه بر این قابلیت ها و توانایی های IT به سبک غیر ابری سنتی مدیریت شده است. عملکرد ابزارهای تلفیق سرویس ابری برای یکپارچه سازی IT خانگی موجود با توجه به سرویس های ابری مصرف شده از تأمین کننده سرویس ابری مورد نیاز است [۱، ۷، ۸].

تأمین کننده سرویس ابری مسئولیت ارائه خدمات ابری برای مشتریان این خدمات را دارا است. آن خدمات توسط سکوی مشترک مدیریت ابری<sup>۲</sup> چه با اجرای زیرساخت CCMP یا مصرف یک مورد به عنوان سرویس ارائه می گردند. سرویس های ابری هر نوعی از قابلیت IT تأمین شده توسط تأمین کننده سرویس ابری برای مشتریان خدمات ابری را نمایش می دهند. این خدمات خصوصیات ابری شامل سرویس مبتنی بر تقاضا، دسترسی شبکه ای گسترده، جمع آوری منابع، انعطاف سریع و سرویس اندازه گیری شده را در برمی گیرد [۸].

<sup>۲</sup> CCMP

لایه های JaaS، PaaS و SaaS توسط NIST تعریف شده است و BPaaS توسط IBM منتشر شده است. از این رو، خدمات فرایند کسب و کار هرگونه فرایند شغلی ارائه شده از طریق مدل سرویس ابری است [۸].

سکوی مشترک مدیریت ابری مجموعه ای از خدمات پشتیبان عملیاتی و خدمات پشتیبان کسب و کار را به معرض نمایش می گذارد. همچنین شامل سطوح کاربری است که سه نقش اصلی تعریف شده در مرجع رایانش ابری را ایفا می کند. این سه نقش اصلی شامل موارد ذیل است [۷، ۸]:

- پورتال مشتری خدمات که به وسیله مشتریان خدمات ابری برای ارائه سرویس و مدیریت مورد استفاده قرار می گیرد.
- پورتال تأمین کننده سرویس که در جهت منافع مدیران تأمین کننده عمل می کند تا حامی عملیات تولید باشد و پورتال پیشبرد بکار رفته توسط سازندگان سرویس ابری.
- خدمات پشتیبانی عملیاتی مجموعه ای از مدیریت عملیاتی و سرویس های مرتبط تخصصی نمایش داده شده توسط CCMP را بیان می کند. از این رو مورد نیاز سازندگان خدمات ابری به منظور راه اندازی سرویس ابری است.

#### ۱.۴. ساختارهای امنیتی رایانش ابری

ساختار و مکانیزم های امنیتی، از ویژگی های کلیدی در رایانش ابری است. این مفاهیم در راستای تحقق رسیدن به یک سرویس امن در رایانش ابری، کمک بلقوه ای خواهند کرد. شش عنصر کلیدی برای مدیران و سازمان های فناوری اطلاعات برای ساخت یک اکوسیستم ابر قابل اعتماد کمک می کند. سازمان ها باید این اکوسیستم رو درک کرده و ویژگی های یک اکوسیستم ابر قابل اعتماد را درک کنند و دستورالعمل های سازمان ها بر پایه این مدل باید ارائه شود. ساختن اعتماد در ابر نیاز به این دارد که به محیط ابری خودتان را ایجاد کنید. شکل ۲ این اکوسیستم را نشان داده است [۳، ۹].



شکل ۲ - اکوسیستم ابر قابل اعتماد [۹]

مباحث امنیتی رایانش ابری در ۸ بخش می تواند تقسیم بندی شود. این ۸ بخش شامل مفاهیم ذیل است. جدول ۲ به بررسی این ۸ فاکتور پرداخته است [۳].

- ذخیره سازی داده و محاسبه مسائل امنیتی
- مجازی سازی مسائل امنیتی
- اینترنت و خدمات مرتبط با مسائل امنیتی
- مسائل امنیتی شبکه
- مسائل کنترل دسترسی

- مسائل امنیت نرم افزاری
- مسائل مدیریت اعتماد و جنبه های انطباق و قانونی

جدول ۲ - بررسی مباحث امنیتی در رایانش ابری

نوع	توضیحات
ذخیره سازی داده و محاسبه مسائل امنیتی	موضوع ذخیره سازی داده، محاسبه غیر اعتماد، دسترسی داده و سرویس، رمزنگاری، بازیافت داده ابری و بدافزار
مجازی سازی مسائل امنیتی	مدیریت پشتیبانی ماشین مجازی، ناظر ماشین مجازی، مجازی سازی شبکه، سیار بودن، مسائل مربوط به ماشین مجازی و بدافزار
اینترنت و خدمات مرتبط با مسائل امنیتی	تهدیدات پیشرفته مکرر و خطرناک، پروتکل های اینترنت، سرویس های وب، تکنولوژی های وب و دسترسی سرویس
مسائل امنیتی شبکه	سکوها ی موبایل و امنیت محیط
مسائل کنترل دسترسی	دسترسی فیزیکی، اعتبارنامه های کاربر، تصدیق سازمان، مجوز، مدیریت هویت کاربر و ناشناس شدن
مسائل امنیت نرم افزاری	سکو و چارچوب ها و پیشروی کاربر
مسائل مدیریت اعتماد	ابر نسبت به اعتماد ابر، جنبه انسانی، شهرت، اعتماد طبق گزارش های ممیزی و ناشناس شدن
جنبه های انطباق و قانونی	علوم قوانین مهم، قوانین، مسائل قانونی، سنجش مصرف نادرست و هدایت

همچنین، مهم ترین مسائل مهم امنیت و حریم خصوصی در جدول ۳ بررسی شده است. جدول ۳ خلاصه ای از آن مقولات و توصیه های مرتبط برای سازمان ها را ارائه می دهد تا در زمان طرح ریزی، مرور، مذاکره یا آغاز مناسبات برون دادی سرویس ابری عمومی رعایت کند [۹].

جدول ۳ - بررسی مسائل امنیتی و حریم خصوصی

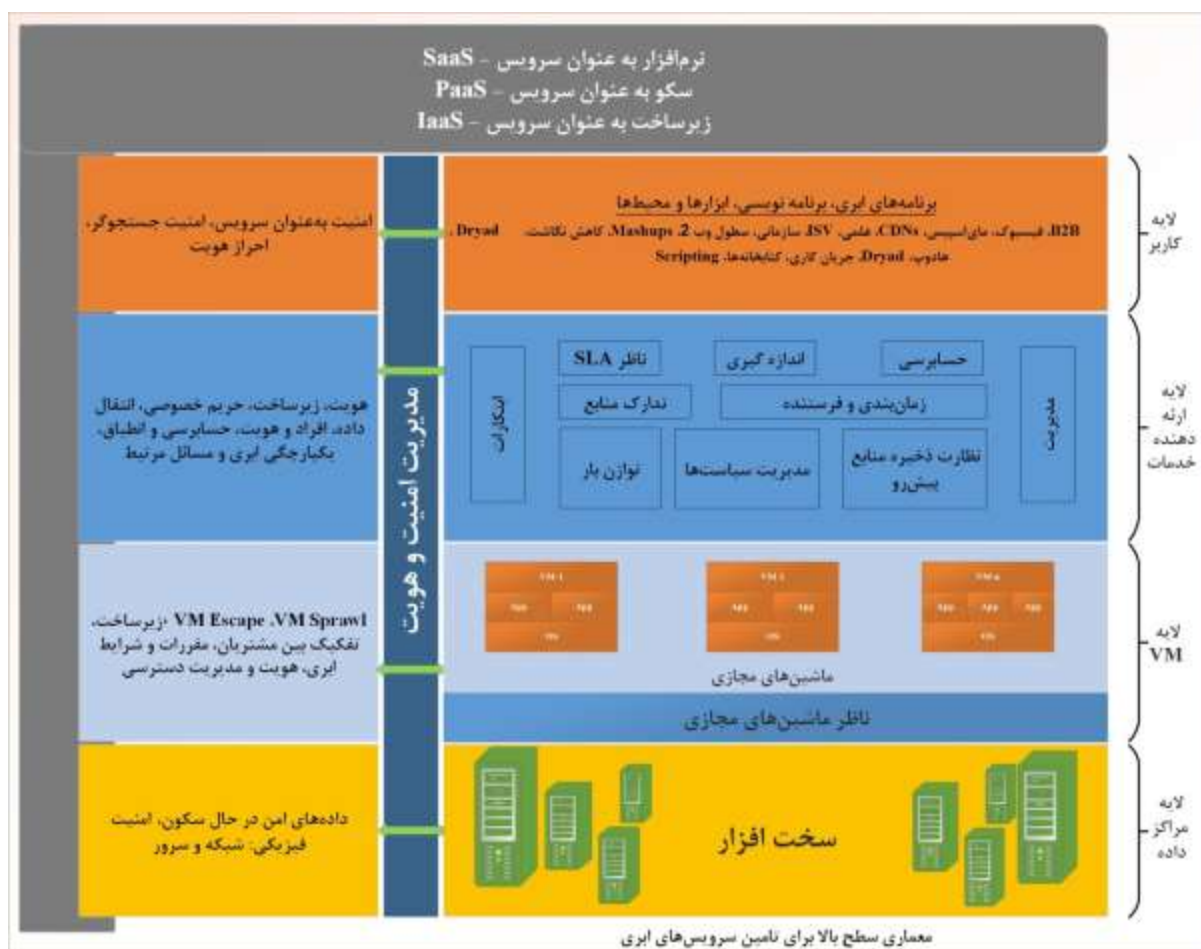
نواحی	توصیات
دولت	گسترش دادن امورات سازمانی مربوط به خط مشی ها و روندهای اجرایی و استانداردهای بکار رفته برای توسعه برنامه کاربردی و تدارک سرویس در ابر، همچنین، طراحی، پیاده سازی، آزمون، کاربری، و نظارت سرویس های مورد استفاده یا مربوطه. بکارگیری مناسب ابزارها و مکانیزم بازرسی برای تضمین امورات سازمانی در سراسر چرخه عمر سیستم.
پذیرش	درک انواع مختلفی از قوانین و مقرراتی که الزامات امنیت و حریم خصوصی را در سازمان اعمال می کند و بطور بالقوه اقدامات محاسبات ابری، بالاخص آنهایی که مربوط به موقعیت مکانی داده، کنترل های امنیتی و حریم خصوصی، مدیریت سوابق، و الزامات کشف الکترونیک را تحت تأثیر قرار می دهند.



مرور و ارزیابی راهنمایی ها و پیشنهاد های ایجادگر ابری با توجه به الزامات سازمانی برای انجام آنها و تضمین اینکه مفاد قرارداد بطور دقیق آن الزامات را تأمین می کند .	
اعتماد	تضمین اینکه مناسبات سرویس از ابزاری مکفی برای صدور اجازه قابلیت رؤیت در داخل پروسه ها و کنترل های امنیتی و حریم خصوصی که توسط ایجادگر ابری بکار می رود، و اجرای آنها در طی زمان برخوردارند. تأسیس حقوق مالکیت انحصاری و بی ابهام بر روی داده نهادینه سازی برنامه مدیریت بحران که به حد کافی انعطاف پذیر برای سازگاری دائمی با ظهور و تغییر جهت چشم انداز بحران در چرخه عمر سیستم باشد. نظارت همیشگی و پیوسته حالت امنیت سیستم برای پشتیبانی از تصمیمات پیشرفته مدیریت بحران
معماری	درک فناوریهای تحت امری که ایجادگر ابری از آنها استفاده می کند تا سرویس ها را تدارک بیند ، که شامل دلالتهایی بر کنترل های تکنیکی مربوطه در امنیت و حریم خصوصی سیستم ، کل چرخه عمر سیستم و سراسر اجزای سیستم می شود.
هویت و دسترسی	تضمین اینکه حراست های کافی در موقعیت مناسب حضور داشته باشند تا اعتبار سنجی ، سندیت و سایر عملکردهای مدیریت هویت و دسترسی را امن نمایند ، و متناسب با آن سازمان باشند.
جداسازی نرم افزاری	درک مجازی سازی و سایر فناوری های منطقی جدا سازی که ایجادگر ابری در معماری نرم افزار چند مستأجری اش بکار می گیرد ، و ارزیابی مخاطرات و بحران ها مربوطه به سازمان
پشتیبانی داده	ارزیابی تناسب راه حل های مدیریت بحران ایجادگر ابری با داده سازمانی مربوطه و توانایی کنترل دسترسی به داده ، به منظور حفاظت از داده در مرحله انتقال و مصرف ، و به منظور پاکسازی داده در نظر گیری خطر تلفیق داده سازمانی با داده های سایر سازمان هایی که احتمال تهاجم به پروفایل هایشان بسیار بالاست یا داده هایشان بصورت انباشتی ارزش متمرکز قابل ملاحظه ای را ارائه می دهند . درک کامل وسنجش مخاطرات مربوطه به مدیریت کلیدی کد نویسی با تسهیلات در دسترس محیط ابری و پروسه های احراز شده توسط ایجادگر ابری
دسترس پذیری	درک رویه های اجرایی و تدارکات قراردادی برای دسترس پذیری ، روگرفت داده و بازیابی ، و بازیابی حادثه ، و تضمین اینکه آنها الزامات طرح ریزی احتیاطی و مداومت عملیات سازمان را تأمین می کند . تضمین اینکه طی اختلال طولانی یا متوسط یا فاجعه جدی ، عملیات های بحرانی فوراً ادامه یابند و اینکه تمام عملیات در نهایت به روشی سازمان یافته و به هنگام دوباره برقرار گردد .
پاسخ گویی به یک اتفاق	درک رویه های اجرایی و تدارکات قراردادی برای پاسخ گویی به اتفاقی یا تضمین اینکه آنها الزامات سازمان را تأمین می کنند تضمین اینکه ایجادگر ابری پروسه پاسخگویی شفاف و مناسب ، و مکانیزم های کارا برای اشتراک اطلاعات در طی و بعد از حادثه داشته باشد. تضمین اینکه سازمان به اتفاقات به روشی هماهنگ با ایجادگر ابری برطبق نقش ها ومسئولیت های مربوطه شان برای محیط ابری پاسخ گو باشد.

##### ۵. بررسی و ارائه راهکار معماری امنیتی رایانش ابری

دیدگاه معماری از مسائل امنیتی به منظور بررسی در محیط رایانش ابری و به منظور تأمین امنیت مشتری است. در این رابطه، ۴ لایه مبتنی بر دسته بندی رایانش ابری شناسایی شده است. دسته بندی رایانش ابری مبنی بر سرویسهایی بصورت نرم افزار بعنوان سرویس، سکو بعنوان سرویس و زیرساخت بعنوان سرویس صورت پذیرفته است. این بخش ۴ لایه مشخص در شکل ۳ طراحی مسائل امنیتی متفاوت در هر لایه را شفاف سازی می نماید [۱۰، ۱۱].



شکل ۳ - معماری امنیتی رایانش ابری [۱۰]

با توجه به مسائل بیان شده در زمینه معماری رایانش ابری و بررسی ساختارهای امنیتی در این حوزه، در ادامه به بررسی کارهای پژوهشگران در زمینه معماری امنیتی رایانش ابری پرداخته شده است. همچنین، جدول ۴ به بررسی کامل معماری - های امنیتی رایانش ابری و ارائه راهکارهایی برای بهبود در حوزه دفاعی پرداخته است.

رایانش ابری (ابر) به طور گسترده‌ای برای ذخیره و پردازش داده‌های بزرگ (کلان داده) <sup>۳</sup> مورد استفاده قرار می‌گیرد. بسیاری از محققان در تلاش برای محافظت و بهبود داده‌های بزرگ در محیط رایانش ابری هستند. مکانیزم‌های سنتی امنیتی با استفاده از رمزنگاری به منظور محافظت داده‌های بزرگ در ابرها، ناکارآمد و نامناسب هستند. در این مقاله، ابتدا درباره چالش‌ها و راه‌حل‌های بالقوه برای محافظت از داده‌های بزرگ در رایانش ابری بحث شده است. دوم؛ این مقاله یک معماری امنیتی مبتنی بر رایانش ابری به نام معماری MetaCloudDataStorage برای محافظت از داده‌های بزرگ پیشنهاد داده است. این معماری بر پایه‌ی یک چارچوب جهت پردازش کارآمد داده‌های بزرگ در محیط رایانش ابری را تضمین می‌کند. از - این‌رو، سازمان‌ها و ارائه دهندگان خدمات ابری در زمینه کسب و کار توسعه بیشتری را به دست می‌آورند [۱۲].

همچنین در این مقاله از چارچوب Map Reduce برای پیدا کردن تعداد کاربرانی که به مرکز داده ابری وارد شده‌اند، استفاده شده است. چارچوب پیشنهادی با استفاده از رابط MetaCloudDataStorage به هر ارائه‌دهنده ابری، نگاشتی از

<sup>۳</sup> Big Data

عناصر داده‌های مختلف را نشان داده و محافظت می‌کند. با توجه به نظرات محققین این مقاله، این رویکرد پیشنهادی نیاز به تلاش زیادی در زمینه پیاده سازی دارد، اما اطلاعات ارزشمندی برای رایانش ابری محسوب می‌شود که می‌تواند بر سیستم‌های نسل آینده تاثیر بگذارد. به عنوان یک کار برای آینده این طرح این است که معماری MetaCloudDataStorage از جریان داده‌ها برای پردازش زمان واقعی گسترش پیدا کند [۱۲].

این مقاله یک چارچوب تطبیق‌دهنده رایانش ابری<sup>۴</sup> مبتنی بر امنیت سازگار برای ابرهای کسب‌وکار را ارائه داده است. معماری CCFA از چندین لایه امنیتی براساس توسعه و یکپارچگی ساخته شده است. همچنین از سه تکنولوژی امنیتی: فایروال، مدیریت احرازهویت و رمزنگاری بر اساس توسعه همگام سازی فایل سازمانی و به اشتراک گذاری فناوری‌ها در راستای ایجاد یکپارچگی و توسعه استفاده کرده است. در این مقاله هسته فناوری‌ها به تفصیل توضیح داده شده‌اند و آزمایش‌ها برای نشان دادن استحکام امنیتی چند لایه معماری CCAF طراحی شده‌اند. در آزمایش نفوذ صورت گرفته در این مقاله، امنیت چند لایه CCAF می‌تواند ۹۹٫۹۵٪ ویروس‌ها و تروجان‌ها را شناسایی و مسدود سازد. تشخیص و مسدود کردن زمان شناسایی ویروس‌ها و بدست آوردن زمان برای حملات مسدود شده در این آزمایش موفق بوده است. معماری چندلایه CCFA پیشنهادی به طور کامل می‌تواند حملات تزریق SQL را متوقف کرده و داده‌ها را به صورت دقیق و واقعی محافظت کند. همچنین این معماری هیچ پیغام اشتباهی را گزارش نمی‌کند. دقت معماری پیشنهادی این مقاله در آزمایش‌های صورت گرفته، ۹۹٫۷۵ درصد است. مکانیسم ترکیبی معماری چندلایه امنیتی CCAF با سیاست، خدمات واقعی و فعالیت‌های تجاری نشان داده شده است. ایده‌های این معماری می‌تواند حجم، سرعت و خدمات کلان داده در ابرها تضمین کند و همچنین برای امنیت رایانش ابری مفید باشد. با توجه به بررسی‌های انجام شده، این مقاله یک رویکرد امنیتی یکپارچه بر اساس معماری پیشنهادی چند لایه امنیتی CCAF را نشان داده است. این پژوهش برای نشان دادن معماری امنیتی چند لایه CCAF به عنوان یک چارچوب کاری برای ابرهای تجاری، آزمایشات و طراحی بررسی شده است. به عنوان کار آینده این مقاله پیشنهاد داده است که یک همکاری بین المللی از طرف خود با شرکای کشورهای مختلف تقویت کنند و اثبات‌های متفاوتی از مفاهیم، نمونه‌های اولیه، خدمات و مشاوره تحقیقاتی را با همکاران مشابه‌شان ایجاد کنند [۱۳].

چگونگی اطمینان از امنیت شبکه برای ماشین‌های مجازی مدرت مبتنی بر سکوها رایانش ابری، هنوز هم یک سوال مبهم و بی پاسخ است. جواب دادن به این سوال مهم به توسعه رایانش ابری در سال‌های اخیر و آینده کمک خواهد کرد. اگرچه در سال‌های اخیر راه‌حلی به صورت ناقص (نادیده گرفتن ویژگی‌های مهم رایانش ابری) ارائه شده است. در این مقاله، یک معماری امنیتی شبکه برای رایانش ابری<sup>۵</sup> مبتنی بر ویژگی‌های آن ارائه شده است. به طور مشخص [۱۴]:

- ۱) حفاظت از ترافیک داخلی و خارجی را در محاسبات ابری فراهم می‌کند (حفاظت از حملات داخلی و خارجی)
- ۲) با توجه به بارگذاری مجدد مجازی باعث مقیاس پذیری قابل انعطاف می‌شود (مقایس پذیری انعطاف‌پذیر)
- ۳) بدست آوردن تحمل خطا بین خطاهای موجود در مجازی سازی (قابلیت موثر در تحمل خطا)

نتایج و آزمایش‌ها از نمونه اولیه معماری NetSecCC نشان داده است که این معماری موثر با سربار کاری کم است و می‌توان آن را جهت ارتقاء گسترده‌ای در رایانش ابر پیاده‌سازی کرد. از این رو، این مقاله یک معماری جهت اطمینان از امنیت شبکه در رایانش ابری را پیشنهاد کرده است. معماری پیشنهادی NetSecCC به طور مشخص سه نقطه ضعف اشاره شده را بهبود داده است. این معماری توانسته یک حفاظت و امنیت جامعتری را برای رایانش ابری فراهم می‌کند. از این رو در آینده می‌توان تحقیقاتی امنیتی تحت شبکه رایانش ابری انجام داد [۱۴].

امنیت یک نگرانی اساسی در رایانش ابری است. تعدادی از ارائه دهندگان خدمات ابری، برای توصیف سطح امنیتی خدمات خود، معماری مرجع امنیتی (SRAs) را پیشنهاد کرده‌اند. معماری SRA یک معماری انتزاعی بدون جزئیات اجرایی است که

<sup>۴</sup> CCAF

<sup>۵</sup> NetSecCC

یک مدل مفهومی امنیت برای سیستم ابری را نشان می دهد. به طور کلی، معماری ارجاع (RAS) در حال تبدیل شدن به ابزار مفیدی برای درک و ساخت سیستم های پیچیده است. این مقاله یک معماری مرجع امنیتی (SRA) ارائه کرده است که با استفاده از مدل ها و الگوهای UML تعریف شده است. همچنین، یک رویکرد خاص برای ساختن سیستم های ایمن را در برمی گیرد. این مقاله یک مدل افزوده و یک الگوی قابل اجرا را ارائه کرده است که این رویکرد را مفهومی کرده اند. برخی از کاربردهای SRA شامل ارزش های SLA، گواهی خدمات و نظارت و ارزیابی امنیتی است که این مقاله این جزئیات را نشان داده است. به همین دلیل برای ساخت یک معماری مرجع امنیتی قوانین و جزئیاتی نیاز است. که این جزئیات میتواند باعث کاهش هزینه و توسعه سیستم های ابری شود [۱۵]:

- یک راه برای درک یک سیستم پیچیده مانند یک ابر امن
- نمای کلی امنیتی
- راهی برای متحد کردن اصطلاحات ابر
- انتخاب ارائه دهندگان ابر بر اساس الزامات امنیتی
- توافقنامه سطح خدمات (SLA)
- گواهی خدمات
- ارزیابی امنیتی
- مدیریت امنیت
- واسطه ابری
- یکپارچگی انواع دستگاه ها
- فدراسیونی از چندین ابر

این مقاله معتقد است که SRA بسیار مهم هستند و برای بهبود امنیت رایانش ابری باید مورد تحقیق قرار گیرند. تهیه مراجع خوب برای الگوهای امنیتی بسیار مهم است که به طراحان و معماران کمک می کند تا از معماری مرجع برای اضافه کردن امنیت و ارزیابی امنیت رایانش ابری و نیز ساختن SLA استفاده کنند [۱۵].

جدول ۴ - بررسی و ارائه راهکارهایی جهت بهبود معماری امنیتی رایانش ابری در حوزه دفاعی

مرجع	معماری پیشنهادی	نقاط قوت و ضعف	راه کارهای توسعه پیشنهادی
[۱۲]	یک معماری امنیتی مبتنی بر رایانش ابری به نام معماری MetaCloudDataStorage بر پایه ی چارچوب Map Reduce.	محافظت از داده های بزرگ. پردازش کارآمد داده های بزرگ. پیدا کردن تعداد کاربرانی که به مرکز داده ابری وارد شده اند.	از جریان داده ها برای پردازش زمان واقعی گسترش پیدا کند.
[۱۳]	یک چارچوب تطبیق دهنده رایانش ابری (CCAF) مبتنی بر امنیت سازگار برای ابرهای کسب و کار. همچنین از سه تکنولوژی امنیتی: فایروال، مدیریت احراز هویت و رمزنگاری استفاده کرده است.	شناسایی و مسدود ۹۹,۹۵٪ ویروس ها و تروجان ها. تشخیص و مسدود کردن زمان شناسایی ویروس ها و بدست آوردن زمان برای حملات مسدود شده در این آزمایش موفق بوده است.	تقویت یک همکاری بین المللی از طرف خود با شرکای کشورهای مختلف و ایجاد اثبات های متفاوتی از مفاهیم، نمونه های اولیه، خدمات و مشاوره تحقیقاتی.
[۱۴]	یک معماری امنیتی شبکه برای رایانش ابری (NetSecCC) با	حفاظت از حملات داخلی و خارجی.	تحقیقاتی امنیتی تحت شبکه رایانش ابری.

	توجه به ویژگی های رایانش ابری.	مقایس پذیری انعطاف پذیر. قابلیت موثر در تحمل خطا.	
[۱۵]	یک معماری انتزاعی به نام SRA بدون جزئیات اجرایی که یک مدل مفهومی امنیت برای سیستم ابری را نشان می دهد.	کاهش هزینه و توسعه سیستم های ابری. متحد کردن اصطلاحات ابری. یکپارچگی انواع دستگاه ها.	تهیه مراجع خوب برای الگوهای امنیتی
[۱۶]	نرم افزار را بصورت یک سرویس ابری سازمانی (SaaS) تحلیل نموده و موقعیت تحقیقی از مشکلات امنیتی را در محیط رایانش ابری معرفی می کند.	پشتیبانی از تحقیقات بعدی نسل سیمار از راه حل ها. هدایت بکارگیری سیاست های امنیتی سرویس های ابری سازمانی SaaS.	سرویس های رایانش ابری سازمان بیشتر به امنیت اطلاعاتی ارائه شده توسط کاربران توجه دارند، از ایم رو باید بر مقوله مقیاس پذیری بیشتر توجه شود.
[۱۷]	یک معماری مبتنی بر سکو به عنوان سرویس (PaaS) مورد اعتماد جهت توسعه امنیت.	بهبود امنیت داده و تهدیدات حریم خصوصی. قابل اعتماد برای پایگاه داده های شخصی.	این مدل باید با پروتکل های امنیتی مختلف بررسی شود و همچنین با سیاست های کنترل دسترسی یکپارچه شود.
[۱۸]	یک طرح مبتنی بر رمزنگاری کارآمد، قابل دسترس و قابل انعطاف.	در قبال تغییرات در اطلاعات و ناامنی در اطلاعات به خوبی عمل می کند. این طرح مقیاس پذیر و انعطاف پذیر است.	استفاده از رمزنگاری مبتنی بر مفاهیم کوانتومی برای بهبود امنیت.
[۱۹]	این مقاله به عنوان یک چارچوب معماری امنیتی سعی در حل تقسیم مسئولیت ها بر اساس الزامات امنیتی در معماری رایانش ابری را دارد.	تقسیم بندی مسئولیت ها و انعطاف پذیری در راستای سیاست های امنیتی سازمان	از نیازهای ضروری این طرح برای آینده کاهش هزینه ها و پردازش های اضافی محاسبات است
[۲۰]	یک سرور سخت افزار افزایشی برای کمک جهت حفاظت از کدها و داده.	از بین بردن نیاز به یک لایه مجازی سازی در طول زمان اجرا مجازی ماشین. بهبود سخت افزار. مدیریت پویا منابع سرور. افزایش اعتماد صحت معماری های سخت افزاری و نرم افزاری و تسهیل ارتقاء طراحی به سخت افزار.	بهبود مقوله هایی همانند بسیاری از سیستم های اصلی وقفه، بهبود سرعت و زمان سیستم، بهبود دستورالعمل های محرمانه و بهبود واسط برای سخت افزارهای مجازی. توسعه پارامترهایی نظیر اتوماتیک کردن تائید امنیتی، گسترش این مقوله در برابر انواع حملات و ترکیب پروتکل ها.
[۲۱]	یک معماری سیستم ابری جدید به نام CypherDB، برای حفاظت از محرمانه بودن پردازش برون سپاری	می تواند توسط یکپارچگی با SQLite، یک برنامه کاربردی پایگاه داده کاربردی قابل اعتماد	پژوهش در مقوله هایی همانند معماری چندهسته ای، برنامه کاربردی هدف یافته، پشتیبانی از

پایگاه داده	باشد.	کامپایلرها، سوئیچ کردن مبتنی بر متن و حفاظت از حملات تزریق کد در بهبود امنیت رایانش ابری.
	مقرون به صرفه و دارای عملکرد (کارایی) بالا.	

## ۶. نتیجه گیری

رایانش ابری سرویس بروی اینترنت با منابع مقیاس پذیر دینامیک ارائه می دهد. تهیه کنندگان سرویس رایانش ابری، مزایایی برای کاربران از نظر هزینه و برنامه های مهمی برای محیط های ابری مشترک و عمومی تامین می کند. محیط های ابری، مقیاس پذیری بالایی برای پردازش داده و نیازهای ذخیره سازی دارند. محیط رایانش ابری مزایا و معایب متعددی از لحاظ امنیت داده ای کاربران سرویس دارد. به همین دلیل اصول امنیت ابر طبق معماری رایانش ابری طبقه بندی می گردد. به همین دلیل، این مقاله در راستای بهبود معماری سازمان های امنیتی، به بررسی و ارائه راهکارهایی جهت توسعه معماری امنیتی رایانش ابری پرداخته است.

## مراجع

۱. Mell, P., & Grance, T. (۲۰۱۱). The NIST definition of cloud computing.
۲. Erl, T., Puttini, R., & Mahmood, Z. (۲۰۱۳). *Cloud computing: concepts, technology & architecture*. Pearson Education.
۳. Carlin, S., & Curran, K. (۲۰۱۳). Cloud computing security. In *Pervasive and Ubiquitous Technology Innovations for Ambient Intelligence Environments* (pp. ۱۲-۱۷). IGI Global.
۴. Zhang, H., Han, W., Lai, X., Lin, D., Ma, J., & Li, J. (۲۰۱۵). Survey on cyberspace security. *Science China Information Sciences*, ۵۸(۱۱), ۱-۴۳.
۵. Badger, L., Bernstein, D., Bohn, R., De Vault, F., Hogan, M., Iorga, M., ... & Sokol, A. (۲۰۱۴). US government cloud computing technology roadmap. US Department of Commerce, National Institute of Standards and Technology.
۶. Zhao, W., Peng, Y., Xie, F., & Dai, Z. (۲۰۱۲, November). Modeling and simulation of cloud computing: A review. In *۲۰۱۲ IEEE Asia Pacific cloud computing congress (APCloudCC)* (pp. ۲۰-۲۴). IEEE.
۷. Jadeja, Y., & Modi, K. (۲۰۱۲, March). Cloud computing-concepts, architecture and challenges. In *۲۰۱۲ International Conference on Computing, Electronics and Electrical Technologies (ICCEET)* (pp. ۸۷۷-۸۸۰). IEEE.
۸. Stifani, R. A. F. F. A. E. L. E., Pappe, S. T. E. F. A. N., Breiter, G. E. R. D., & Behrendt, M. I. C. H. A. E. L. (۲۰۱۲). Ibm cloud computing reference architecture. IBM Academy of Technology, ۳(۱), ۱-۱۶.
۹. Popović, K., & Hocenski, Ž. (۲۰۱۰, May). Cloud computing security issues and challenges. In *The ۳۳rd International Convention MIPRO* (pp. ۳۴۴-۳۴۹). IEEE.
۱۰. Okuhara, M., Shiozaki, T., & Suzuki, T. (۲۰۱۰). Security architecture for cloud computing. *Fujitsu Sci. Tech. J.*, ۴۶(۴), ۳۹۷-۴۰۲.
۱۱. Chen, J., Wang, Y., & Wang, X. (۲۰۱۲). On-demand security architecture for cloud computing. *Computer*, ۴۵(۷), ۷۳-۷۸.
۱۲. Manogaran, G., Thota, C., & Kumar, M. V. (۲۰۱۶). MetaCloudDataStorage architecture for big data security in cloud computing. *Procedia Computer Science*, ۸۷, ۱۲۸-۱۳۳.
۱۳. Chang, V., Kuo, Y. H., & Ramachandran, M. (۲۰۱۶). Cloud computing adoption framework: A security framework for business clouds. *Future Generation Computer Systems*, ۵۷, ۲۴-۴۱.

۱۴. He, J., Dong, M., Ota, K., Fan, M., & Wang, G. (۲۰۱۶). NetSecCC: A scalable and fault-tolerant architecture for cloud computing security. *Peer-to-Peer Networking and Applications*, ۹(۱), ۶۷-۸۱.
۱۵. Fernandez, E. B., & Monge, R. (۲۰۱۴, April). A security reference architecture for cloud systems. In *Proceedings of the WICSA ۲۰۱۴ Companion Volume* (p. ۳). ACM.
۱۶. Niu, D. D., Liu, L., Zhang, X., Lü, S., & Li, Z. (۲۰۱۶). Security analysis model, system architecture and relational model of enterprise cloud services. *International Journal of Automation and Computing*, ۶(۱۳), ۵۷۴-۵۸۴.
۱۷. Niu, D. D., Liu, L., Zhang, X., Lü, S., & Li, Z. (۲۰۱۶). Security analysis model, system architecture and relational model of enterprise cloud services. *International Journal of Automation and Computing*, ۶(۱۳), ۵۷۴-۵۸۴.
۱۸. Gupta, S. K., Rawat, S., & Kumar, P. (۲۰۱۴, October). A novel based security architecture of cloud computing. In *Reliability, Infocom Technologies and Optimization (ICRITO)(Trends and Future Directions)*, ۲۰۱۴ ۳rd International Conference on (pp. ۱-۶). IEEE.
۱۹. Drozdova, M., Rusnak, S., Segec, P., Uramova, J., & Moravcik, M. (۲۰۱۷, October). Contribution to cloud computing security architecture. In *Emerging eLearning Technologies and Applications (ICETA)*, ۲۰۱۷ ۱۵th International Conference on (pp. ۱-۶). IEEE.
۲۰. Szefer, J. M. (۲۰۱۳). Architectures for secure cloud computing servers (Doctoral dissertation, Princeton University).
۲۱. Chen, H. K. (۲۰۱۶). A novel architecture for secure database processing in cloud computing. HKU Theses Online (HKUTO).